Perancangan *Security Information and Event Management* (SIEM) Menggunakan *Open Source SIEM* (OSSIM)

[1)]Hanief Eko Ardiyanto, [2)]Teguh Indra Bayu

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo, Salatiga 50714, Indonesia
Email : [1)]672014103@student.uksw.edu, [2)] teguh.bayu@uksw.edu

Abstract

The role of network security is very important, one of which is to monitor network connections to guard against manipulation and internal and external attacks. A good network security helps to minimize the risks related to security such as the attacks from outside or inside in the order to corrupting, manipulation of access rights, and provide monitoring for the client on one network. With a centralized SIEM as OSSIM, OSSIM can perform network security protection and monitoring network, send alerts via email, and OSSIM can make the report and send the results to the email. With the email alert and report features, are expected to speed up the prevention process and handling if an attack or problem occurs in the network that requires a fast response.

Keywords : OSSIM, *email alert, report*

Abstrak

Peran keamanan jaringan sangat penting, salah satunya sebagai *monitor* koneksi jaringan untuk menjaga dari penyalahgunaan, serangan dari luar maupun dalam, dan sebagainya. Keamanan jaringan yang baik membantu meminimalisir risiko-risiko yang berhubungan dengan keamanan seperti serangan dari luar maupun dalam yang bertujuan untuk merusak, penyalahgunaan hak akses, dan menyediakan *monitoring* untuk kondisi klien pada satu jaringan. Dengan OSSIM sebagai SIEM terpusat, OSSIM dapat melakukan perlindungan keamanan jaringan dan *monitoring* jaringan, mengirim *alert* melalui *email,* serta OSSIM dapat membuat *report* dan mengirim hasil *report* ke *email.* Dengan fitur *email alert* dan *report,* diharapkan dapat mempercepat proses penanggulangan dan penanganan jika terjadi serangan atau masalah di dalam jaringan yang membutuhkan tanggapan yang cepat.

Kata Kunci : OSSIM, *email alert, report*

[1)]Mahasiswa Fakultas Teknologi Informasi Program Studi Teknik Informatika, Universitas Kristen Satya Wacana Salatiga.
[2)] Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga